วิคเตอร์ ชาร์ลี 5.0
โปรแกรมต่อต้านไวรัสครอบจักรวาล

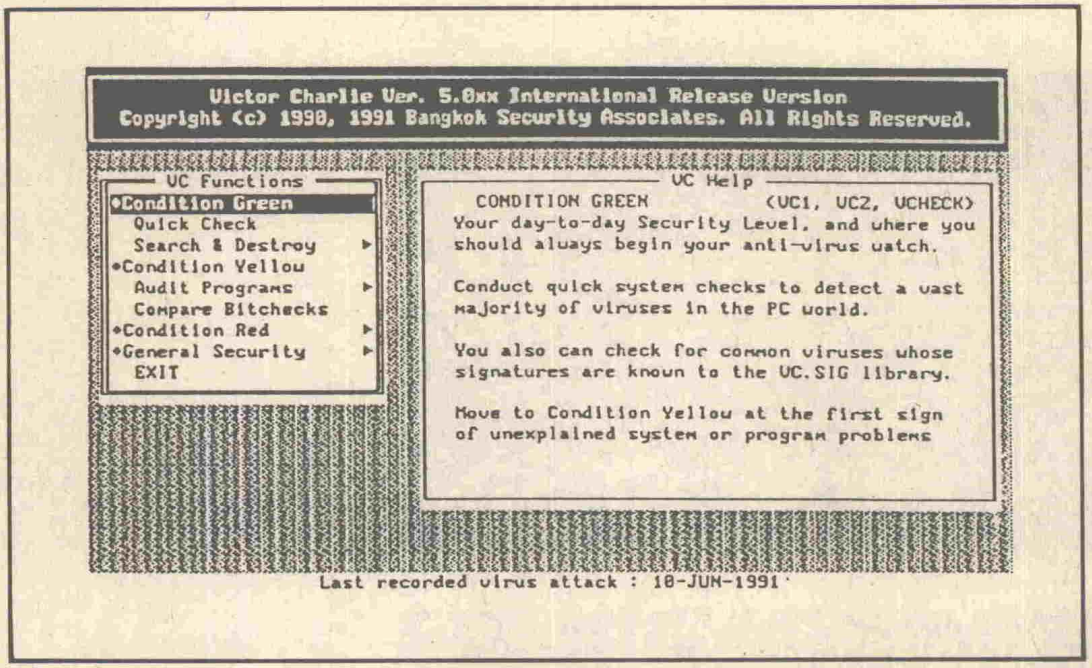
หากต้องการมั่นใจกับข้อมูล
ควรหามาตรการรักษาความปลอดภัย
ป้องกันภัยจากไวรัส

ในช่วงเวลานี้คอมพิวเตอร์เข้ามามีบทบาทในทางธุรกิจ อุตสาหกรรม ราชการ และการทำงานอื่น ๆ และคอมพิวเตอร์มีประโยชน์มากในการทำงานให้มีประสิทธิภาพ ในขณะเดียวกันก็มีภัยอันตรายที่คุกคาม ในการก่อกวนการทำงานของคอมพิวเตอร์ โดยเป็นการรบกวนการทำงานของซอฟต์แวร์ และทำลายข้อมูลที่เก็บอยู่ในเครื่องคอมพิวเตอร์ ซึ่งเราคงจะคุ้นเคยกันดีก็คือ เจ้าไวรัสตัวร้าย เจ้าไวรัสนี้สามารถติดต่อกันระหว่างเครื่องคอมพิวเตอร์ได้ สร้างความเสียหายให้แก่ข้อมูลอันมีค่าของเราไม่น้อยเลย เราไม่ต้องตกใจกันอีกต่อไป เพราะ วิคเตอร์-ชาร์ลี (Victor Charlie) หรือ VC 5.0 สามารถปราบเจ้าไวรัสร้ายนี้ ไม่ให้ทำความเสียหายให้กับระบบคอมพิวเตอร์ของเรา เรามาดูกันว่า วิคเตอร์ชาร์ลีจะช่วยเรากำจัดไวรัสได้อย่างไร

VC 5.0

ซอฟต์แวร์กำจัดและป้องกันไวรัสทั่วไป มักจะใช้วิธีค้นหาอย่างเจาะจง โดยที่มีลายลักษณ์ (Signature) ของไวรัสนานาชนิดเก็บเอาไว้ เพื่อใช้เปรียบเทียบเวลาตรวจหาไวรัสในระบบ ซึ่งปกติจะใช้ได้ผลดีพอสมควร หากแต่ในกรณีที่มีไวรัสเกิดขึ้นมาใหม่โปรแกรมชนิดนี้จะไม่รู้จักไวรัสใหม่ และไม่สามารถกำจัดได้ หากไม่ได้รับการอัพเดตเสียก่อน จากข้อบกพร่องนี้เอง VC จึงได้รับการพัฒนาให้เป็นซอฟต์แวร์ต่อต้านไวรัสชนิดใหม่ที่ใช้หลักการทั่วไป (Generic anti – virus) คือทำการบันทึกสภาพปกติของระบบไว้ตั้งแต่แรก และตรวจสอบจากร่องรอยที่ไวรัสทิ้งไว้ ดังนั้นจึงกล่าวได้ว่าวิคเตอร์ชาร์ลีสามารถตรวจสอบไวรัสได้ครอบจักรวาล

รีวิว
วิคเตอร์ชาร์ลี 5.0
โปรแกรมต่อต้าน
ไวรัสครอบจักรวาล



รูปที่ 1
เมนูของวิคเตอร์ชาร์ลี
ซึ่งมี Help menu
อธิบายการทำงานด้วย

วิคเตอร์ชาร์ลี มีมาตรการหลายอย่างในการจับไวรัส รวมทั้งการตรวจสอบและป้องกันตัวเองด้วย ตัวโปรแกรมประกอบด้วยโปรแกรมหลักและโปรแกรมย่อยเสริมต่าง ๆ อาจจะใช้จากดอส-พรอมพต์ หรือจากระบบเมนูเพื่อความสะดวกก็ได้

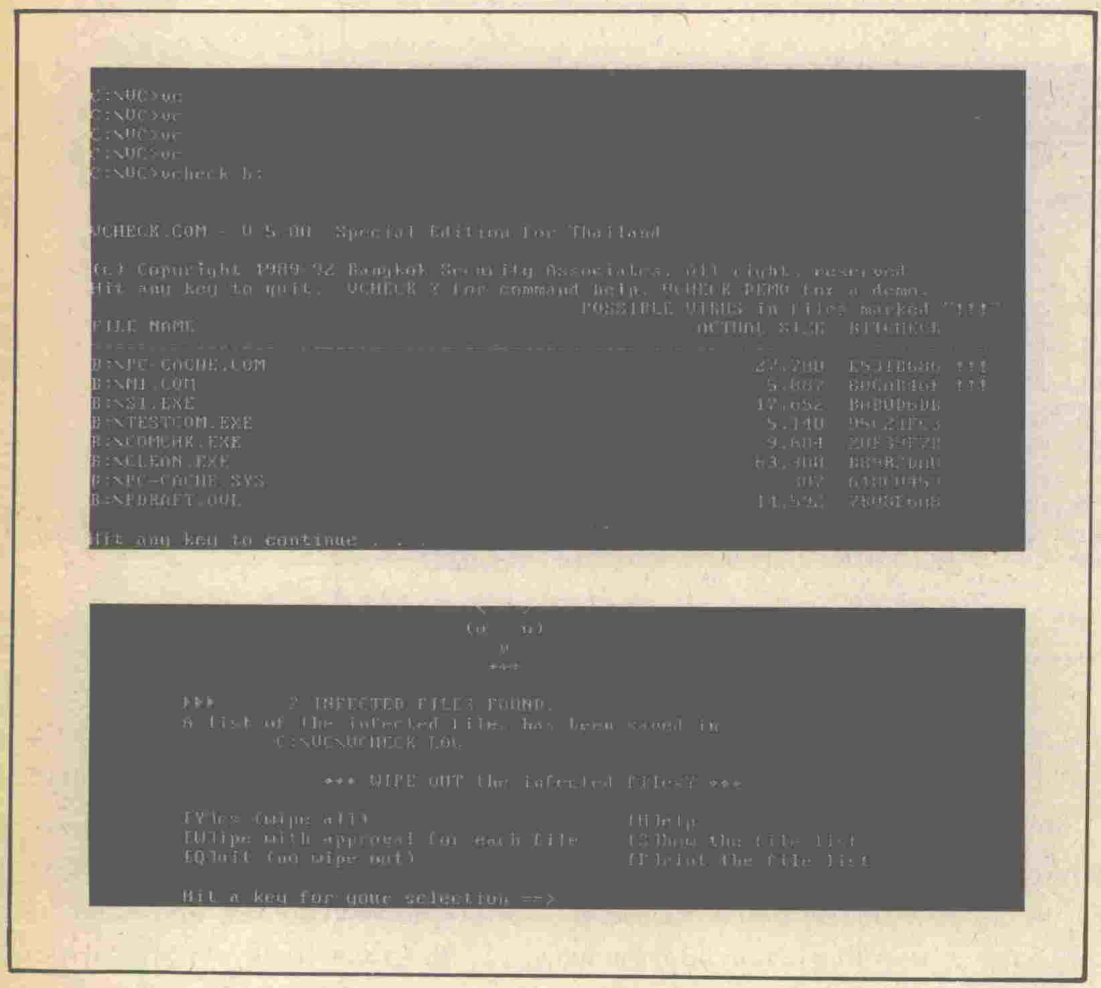
มาตรการการตรวจสอบ

วิคเตอร์ชาร์ลีมีโปรแกรมชื่อ VC1 และ VC2 เป็นด่านหน้า เพื่อล่อให้ไวรัสเข้ามาเกาะ ทันทีที่ไวรัสเข้ามาเกาะ วิคเตอร์ชาร์ลีจะตรวจสอบและจับลายลักษณ์ของไวรัสนั้นเก็บไว้ เพื่อใช้ในการกำจัดไวรัสโดย VCheck ในการติดตั้งนั้น วิคเตอร์ชาร์ลีจะตรวจและจัดเก็บลักษณะของระบบไว้ คือ พาร์ติชันเซกเตอร์, ส่วนบูต, ไฟล์ระบบของดอส, ไฟล์ COMMAND.COM และรายละเอียดของดอสอินเตอร์รัพต์ต่าง ๆ ซึ่งถูกจัดไว้ใน BITCHECK™ เพื่อไว้ใช้เปรียบเทียบกับสิ่งต่าง ๆ ที่จะเปลี่ยนแปลงไปเมื่อถูกไวรัสจู่โจม การตรวจ (scanning) เป็นอีกวิธีหนึ่งซึ่งวิคเตอร์-ชาร์ลีใช้ในการตรวจจับไวรัส โดยใช้การตรวจจับจากลายลักษณ์ของไวรัสทั่วไป โดยใช้โปรแกรม VCHECK ซึ่งได้ผลเหมือนโปรแกรมป้องกันและตรวจจับไวรัสทั่วไป

เริ่มใช้งานกันเสียที

ในการใช้งานวิคเตอร์ชาร์ลีนั้นจะต้องมีการติดตั้งโปรแกรมลงไปบนเครื่องก่อน คือ เป็นการคัดลอกโปรแกรมจากแผ่นต้นฉบับลงบนฮาร์ดดิสก์ โดยใช้โปรแกรม VINSTALL ในแผ่นวิคเตอร์ชาร์ลี จากนั้นก็จะมีการติดตั้ง 2 อย่าง คือ แบบ Quick และ Customized คือ ถ้าเป็นแบบ customized เราจะสามารถเลือกติดตั้งโปรแกรมย่อยได้ตามต้องการ หลังจากติดตั้งเสร็จแล้วจะทำการอินิเชียล เพื่อให้วิคเตอร์ชาร์ลีเก็บข้อมูลของระบบใหม่ทั้งหมด หลังจากนั้นวิคเตอร์ชาร์ลีก็จะคอยปกป้องเตือนภัยเมื่อมีไวรัสเข้ามาทำอันตรายกับระบบ โปรแกรมหลักของวิคเตอร์ชาร์ลีก็จะมี VC.EXE ซึ่งเป็นโปรแกรมที่เรียกใช้โปรแกรมย่อยอื่น โดยสามารถเลือกได้จากเมนู ซึ่งทำให้ทำงานได้อย่างสะดวกและยังมีคำอธิบายการทำงานของแต่ละเมนูให้ดูด้วย ดังรูปที่ 1 วิคเตอร์ชาร์ลีจะแบ่งการทำงานออกเป็น 3 สภาวะ คือ สภาวะเขียว (condition green), สภาวะเหลือง (condition yellow), และสภาวะแดง (condition red)

ในสภาวะเขียวเป็นสภาวะปกติในขณะที่ไม่มีไวรัสเข้ามาทำอะไรกับระบบ คือ จะเป็นการตรวจเช็คไฟล์ต่าง ๆ การตรวจสอบขั้นต้น (Quick check) หรือจะค้นหาไวรัสได้จากการค้นหา และทำลาย (search & destroy) ซึ่งจะสามารถค้นหาไวรัสที่มีลายลักษณ์อยู่ในคลังที่เก็บ สำหรับในสภาวะเหลืองนั้นจะเป็นการทำงานเมื่อมีสิ่งผิดปกติเกิดขึ้นในระบบ โดยจะใช้ BITCHECK ใน



รูปที่ 2
การตรวจจับไวรัส
ประเภทเกาะติดและ
สามารถกำจัดได้ทันที

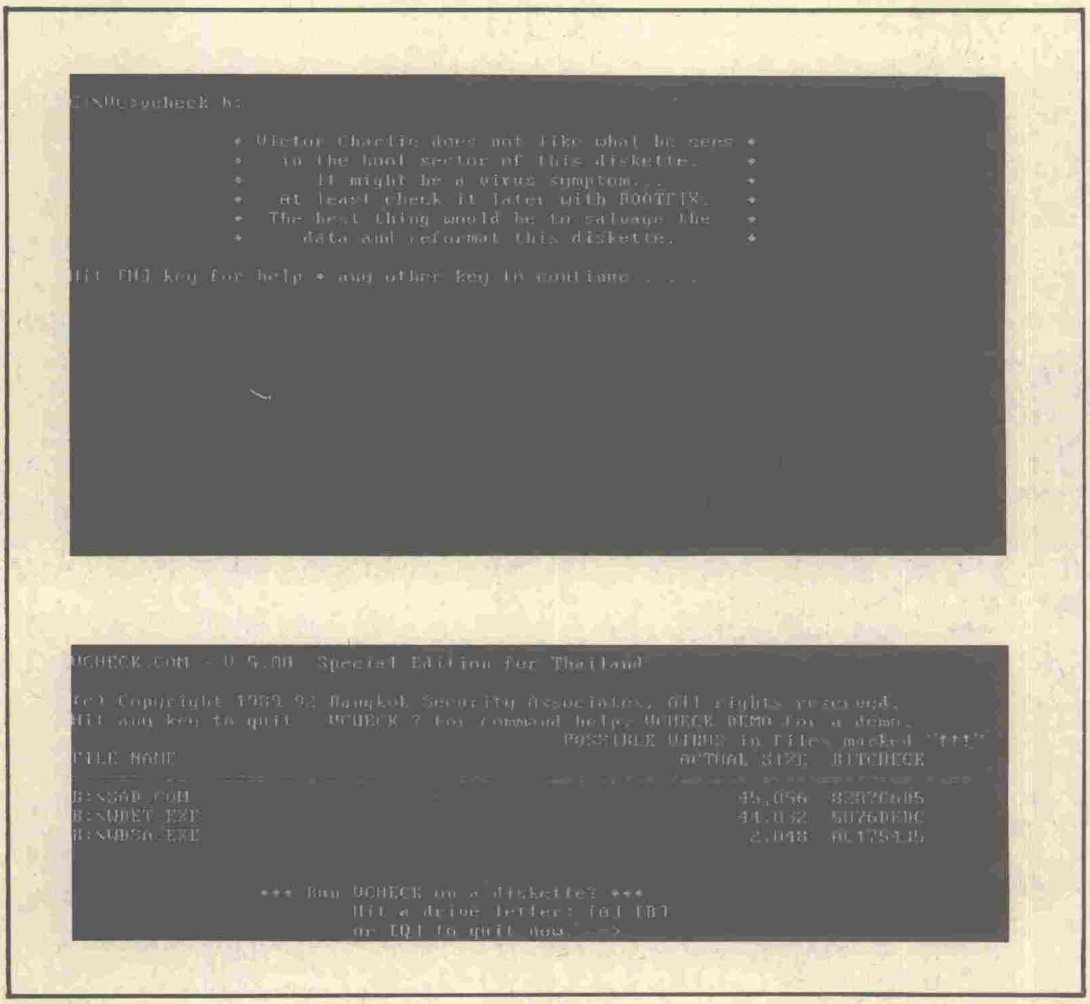
การตรวจสอบที่ละเอียดกว่าสภาวะเขียว และจะรายงานความเปลี่ยนแปลงให้ทราบเมื่อมีสภาวะผิดปกติ ซึ่งทำให้ท่านสามารถจัดการกับไฟล์ที่ผิดปกติได้ทันท่วงที ส่วนในสภาวะแดงนั้นเป็นการกู้ภัยอันเกิดจากการทำลายของไวรัส เป็นการซ่อมส่วนต่าง ๆ เช่น ซ่อมแผ่นดิสค์ที่ติดเชื้อ หรือซ่อมบูตเซกเตอร์ ฯลฯ

เมื่อถูกไวรัสเล่นงาน

เมื่อตรวจพบไวรัสประเภทที่ 1 ซึ่งจะเป็นไวรัสประเภทเกาะติดไฟล์ มีวิธีการกำจัดได้อย่างเดียวก็คือการลบไฟล์นั้นทิ้ง แล้วนำต้นฉบับโปรแกรมมาใช้แทน แต่ต้องแน่ใจว่าไวรัสไม่ได้ติดมาจากโปรแกรมต้นฉบับนั้น โดยการตรวจเช็คโปรแกรมต้นฉบับนั้นว่าปลอดไวรัสจริง ๆ เสียก่อน ในการตรวจวิคเตอร์-ชาร์ลีสามารถตรวจพบไวรัสประเภทนี้ได้เกือบทุกตัว ซึ่งวิคเตอร์ชาร์ลีจะมีลายลักษณ์ของไวรัสเหล่านั้นอยู่แล้ว แต่หากเป็นไวรัสตัวใหม่ซึ่งเข้ามาเกาะติดไฟล์ที่วิคเตอร์ชาร์ลียังไม่มีลายลักษณ์เก็บเอาไว้ มันก็จะต้องใช้ VC1 และ VC2 เป็นตัวล่อ และเก็บลายลักษณ์ของไวรัสตัวใหม่เข้ามาเพื่อใช้ในการตรวจจับต่อไป ในการตรวจก็ใช้จากเมนูเลือกตรวจในไดรฟ์ที่ต้องการดังรูปที่ 2

ไวรัสประเภทที่ 2 ซึ่งเป็นไวรัสที่ซ่อนตัวอยู่ในส่วนบูตเซกเตอร์ ถ้าท่านบูตเครื่องด้วยแผ่นที่ติดไวรัสประเภทนี้ก็จะทำให้ไวรัสแพร่ขยายตัวไปยังดิสค์อื่น ๆ ได้ การตรวจพบนั้นง่ายมาก เพราะทุกครั้งที่วิคเตอร์ชาร์ลีตรวจแผ่นดิสค์ ก็จะตรวจดูบูตเซกเตอร์ด้วย โดยที่ส่วนบูตเซกเตอร์เป็นส่วนที่มีพื้นที่เล็กและการค้นหาก็ง่ายด้วย ดังรูปที่ 3 เมื่อตรวจพบก็สามารถให้วิคเตอร์ชาร์ลีจัดการกับไวรัสนั้น ๆ ได้ทันที โดยการใช้ BOOTFIX

ในการตรวจเช็คไวรัสจะมีไวรัสบางตัวที่หลบซ่อนตัว เมื่อกำจัดไปแล้วไม่หมดอาจจะป้องกันได้โดยการใช้



รูปที่ 3
การค้นหาตรวจจับ
ไวรัสประเภทซ่อนตัว
ในบูตเซกเตอร์

VCHECK d – ซึ่ง d คือชื่อไฟล์ที่ต้องการจะตรวจ และต้องตรวจดูว่าไฟล์โอเวอร์เลย์ต่าง ๆ ที่มีชื่อไม่เหมือนชาวบ้านจะต้องจัดการเปลี่ยนชื่อให้เหมือนกันโดยดูจาก VCHECK.CFG ข้อจำกัดในการตรวจเช็คคือ การค้นหาไวรัสซึ่งติดอยู่ใน compressed file นั้นทำไม่ได้ และนี่อาจเป็นสาเหตุหนึ่งที่ทำให้มีการติดเชื้ออีกเมื่อเอา compressed file ที่ติดเชื้อออกมาใช้ ท่านอาจจะเรียกไฟล์ที่ติดไวรัส หรือสงสัยว่าติดไวรัสออกมาใช้งานเมื่อเสร็จแล้วก็ใช้ VC5 ตรวจสอบ ทำเช่นนี้ไปจนครบทุกไฟล์ที่ต้องการ

ลาก่อนไวรัส

หากข้อมูลของท่านมีความสำคัญกับท่านมาก การสูญเสียข้อมูลไปจึงเป็นเรื่องที่ยอมไม่ได้ การป้องกันไวรัสที่ถูกต้องจะช่วยให้ท่านไม่ต้องมาแก้ไขความเสียหายที่อาจจะแก้ไขไม่ได้นอกจากทำลายทิ้ง การใช้คอมพิวเตอร์หากไม่จำเป็นก็ไม่ควรเอาโปรแกรมหรือแผ่นดิสค์ที่เราไม่แน่ใจ หรือได้มาจากการก๊อบปี้ต่อ ๆ กันมาเพื่อป้องกันการติดเชื้อในเครื่องของท่าน ใช้แต่โปรแกรมที่ท่านแน่ใจว่าปลอดไวรัสก็คือ โปรแกรมที่ซื้อมาจากร้านซอฟต์แวร์อย่างถูกต้อง

อย่างไรก็ดี หากหลีกเลี่ยงการใช้โปรแกรมอื่น ๆ ไม่ได้ก็ต้องหาทางป้องกันเอาไว้ก่อน เพื่อจะได้ไม่ต้องมาปวดหัวกันในภายหลัง วิคเตอร์ชาร์ลีเป็นโปรแกรมต่อต้านไวรัสที่มีความสามารถเหนือกว่าโปรแกรมต่อต้านไวรัสทั่ว ๆ ไป คือ สามารถตรวจจับไวรัสใหม่ ๆ ได้ทันที จึงสามารถที่จะตรวจจับไวรัสได้แบบครอบจักรวาล และช่วยป้องกันและกู้ภัยข้อมูลของเรามิให้ถูกทำลายไป ลาก่อนเจ้าไวรัสตัวร้าย